МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет инновационных технологий

УТВЕРЖДАЮ:
Декан
_____ С. В. Шидловский
«27» августа 2021 г.

Фонд оценочных средств
для изучения учебной дисциплины

Информационные технологии в управлении качеством и защита информации

Направление подготовки
27.03.02 Управление качеством

Профиль подготовки
Управление качеством в производственно-технологических системах

Форма обучения
Очная

Квалификация
Бакалавр

Томск – 2021

Фонд оценочных средств (ФОС) является элементом системы оценивания уровня сформированности компетенций обучающихся, изучающих дисциплину «Информационные технологии в управлении качеством и защита информации».

Целью ФОС является установление соответствия уровня подготовки обучающихся и выпускников требованиям Федерального государственного образовательного стандарта высшего образования по направлению подготовки 27.03.02 Управление качеством (утв. приказом Министерства образования и науки РФ от 9 февраля 2016 г. № 92. С изменениями и дополнениями от: 13 июля 2017 г.).

1. Формируемые компетенции по ФГОС ВО 27.03.02 Управление качеством

Формируемые компетенции *(код компетенции, уровень (этап) освоения)*	**Планируемые результаты обучения по дисциплине**
ОПК-3, III уровень способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**З (ОПК-3) – III Знать:** основные понятия и требования в области информационной безопасности, математические основы методов защиты информации; законодательство в области информационной безопасности **У (ОПК-3) – III Уметь:** выявлять и описывать источники, риски и формы атак на информацию **В (ОПК-3) – III Владеть:** навыками использования широкого круга программ обработки информации (в том числе библиографической), в том числе программы восстановления данных, скрытия данных, установки пароля на некоторые данные и пр.

2. Этапы формирования компетенций в процессе освоения дисциплины

2.1. Лекции

№	Разделы и(или) темы дисциплин	Формируемые компетенции (ОПК-3)	Формы текущего контроля и промежуточной аттестации
1.	Цели и задачи дисциплины. Основные понятия и требования в области информационной безопасности.	+	Текущий контроль: Тест, Контрольная работа Промежуточная аттестация: Тест (итоговый), Контрольная работа (итоговая)
2.	Законодательство в области информационной безопасности	+	
3.	Источники, риски и формы атак на информацию	+	
4.	Поисковые информационные системы	+	Текущий контроль: Контрольная работа Промежуточная аттестация:
5.	Резервное копирование и восстановление данных	+	

6.	Программные средства скрытия данных и установки пароля, очистки данных	+	Контрольная работа (итоговая)
7.	Программы обнаружения и защиты от вредоносных программ	+	
8.	Криптографические методы (математические и программные средства) защиты информации. Электронная подпись (ЭП). Электронные сертификаты	+	Текущий контроль: Тест, Контрольная работа Промежуточная аттестация: Тест (итоговый), Контрольная работа (итоговая)

2.2. Лабораторные работы

№	Разделы и(или) темы дисциплин	Формируемые компетенции (ОПК-3)	Формы текущего контроля и промежуточной аттестации
1.	Формирование политики безопасности	+	Текущий контроль: Отчет по лабораторной работе
2.	Поиск документов в сети Интернет	+	
3.	Восстановление данных	+	
4.	Программные средства информационной безопасности	+	
5.	Настройка безопасности в операционной системе Windows	+	
6.	Антивирусные программные средства обеспечения информационной безопасности	+	
7.	Фаервол	+	
8.	Простейшие алгоритмы шифрования	+	
9.	Симметричные алгоритмы шифрования информации	+	
10.	Асимметричные алгоритмы шифрования информации	+	
11.	Электронная подпись	+	

3. Показатели и критерии оценивания компетенций на различных этапах их формирования

Показатели и критерии оценивания компетенций представлены в картах компетенций Приложение 1

4. Фонд оценочных средств для проведения текущего контроля

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по ее корректировке, а также для совершенствования методики обучения, организации учебной работы.

Текущий контроль включает в себя - контрольную точку 1 и контрольную точку 2.

Контрольная точка 1 проводится в середине семестра и учитывает выполнение лабораторных работ, тестов, посещаемость.

Контрольная точка 2 проводится в конце семестра и учитывает выполнение лабораторных работ, тестов, посещаемость.

Фонд оценочных средств, для проведения текущего контроля включает в себя:

1) Типовые задания для проведения текущего контроля успеваемости по дисциплине (тесты, контрольная работа, отчет по лабораторной работе)

2) Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенции.

4.1. Примеры тестовых заданий фонда оценочных средств

Вопрос 1. Акустический приемник, размещаемый злоумышленником в помещении с конфиденциальной информацией, и радиоэлектронный ретранслятор, обеспечивающий достаточную дальность для съема информации злоумышленником за пределами контролируемой зоны относятся к:

1) Акусторадиоэлектронному каналу утечки информации
2) Акустооптическому каналу утечки информации
3) Акустовещественному каналу утечки информации
4) Электронному каналу утечки информации

Вопрос 2. Статья «создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами» уголовного кодекса записана под номером:

1) 272
2) 273
3) 242
4) 183

Вопрос 3. Преимущества симметричных шифров (по сравнению с асимметричными):

1) Высокая скорость (на 3 порядка быстрее асимметричных)
2) Меньшая требуемая длина ключа для сопоставимой стойкости
3) Хорошая изученность
4) Низкая скорость (на 3 порядка медленнее асимметричных)
5) Нет необходимости передавать ключи по надежному каналу связи

5. Фонд оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся в ТГУ.

Форма промежуточной аттестации – зачет.

Промежуточная аттестация проводится по завершении изучения дисциплины в виде экзаменационной процедуры в устной форме по билетам, которые содержат два теоретических вопроса, направленных на результат «Знать», «Уметь» и «Владеть».

Оценка, выставляемая в зачетную книжку обучающегося и ведомость, складывается из итоговой оценки, полученной за работу в семестре (текущий контроль), и оценки, полученной по итогам промежуточной аттестации.

Фонд оценочных средств, для проведения промежуточной аттестации включает в себя:

1) вопросы к контрольной работе (итоговой) и тесту (итоговому)

2) критерии оценивания

5.1. Вопросы для подготовки к зачету

1. Роль информации и её защиты в современном мире.
2. Определение защиты информации. Значение защиты информации.
3. Аспекты защиты информации.
4. Понятия безопасности информации, безопасности данных и защиты данных.
5. Понятие информационной безопасности.
6. Десять главных угроз защиты информации.
7. Понятия конфиденциальности, целостности и достоверности информации.
8. Понятия доступа к информации, санкционированный и несанкционированный доступ к информации.
9. Понятия идентификации и аутентификации.
10. Понятия угрозы информационной безопасности, уязвимости и атаки.
11. Бернская конвенция, Парижская и Берлинская конференция.
12. Римская и Брюссельская конференция. Всемирная конвенция об авторском праве.
13. Стокгольмская конференция. Особенности присоединения России к международному праву.
14. 3 статьи конституции РФ, связанные с особенностями обработки, хранения и распространения информации.
15. 4 статьи УК РФ, связанные с особенностями обработки, хранения и распространения информации.
16. Органы государственной службы РФ, играющие основную роль в создании правовых механизмов защиты информации.
17. Понятие угрозы. Виды угроз.
18. Классификация источников угроз (перечислить). Антропогенные источники угроз.
19. Классификация источников угроз (перечислить). Техногенные источники угроз.
20. Классификация источников угроз (перечислить). Стихийные источники угроз.
21. Классификация уязвимостей (перечислить). Объективные уязвимости.
22. Классификация уязвимостей (перечислить). Субъективные уязвимости.
23. Классификация уязвимостей (перечислить). Случайные уязвимости.
24. Статистика возникновения умышленных и случайных утечек.
25. Современная система удостоверяющих документов и её недостатки.
26. Бесперспективность защиты носителей и перспективы эволюции удостоверяющих документов.
27. Практика выявления поддельных документов и рекомендации, по защите документов.
28. Классификации каналов утечки информации. Структура канала утечки информации.
29. Оптический канал утечки информации.
30. Акустический канал утечки информации.
31. Радиоэлектронный канал утечки информации.
32. Материально-вещественный канал утечки информации.
33. Понятия криптографического ключа, открытого и закрытого ключа, шифрования, дешифрования и криптоанализа.
34. Понятие симметричного шифрования. Преимущества и недостатки симметричного шифрования. Виды симметричных шифров.
35. Понятие асимметричного шифрования. Преимущества и недостатки асимметричного шифрования. Виды асимметричных шифров.

36. Стандарт DES. Схема шифрования с использованием алгоритма DES. Схема работы одного цикла алгоритма DES.
37. Операционные режимы симметриного шифрования. Режим ECB.
38. Операционные режимы симметриного шифрования. Режим CBC.
39. Операционные режимы симметриного шифрования. Режим CFB.
40. Операционные режимы симметриного шифрования. Режим OFB.
41. "Тройной" DES, Rijndael, RC2.
42. Основные свойства и методы класса Symmetric Algorithm.

5.2. Критерии оценивания

Критерий оценивания для промежуточной аттестации:

В основе оценивания ответов на зачёте лежат принципы объективности, справедливости и всестороннего анализа уровня знаний студентов.

«Зачтено» ставится студенту, у которого выполнены все следующие показатели:

1. Отчеты по всем 11 лабораторным работам зачтены.
2. Освещено не менее чем 70% материала контрольной работы (итоговой). Оценивается: знание фактического материала, а также культура речи, глубина знания, аргументированность ответа, связь теории и практики, умение решить задачу.
3. Получено не менее чем 70 баллов (из 100 возможных) на тест (итоговый).

«Не зачтено» ставится студенту, не имеющему всех трех показателей, описанных выше..